Docket No. AUS920010388US1

ABSTRACT OF THE DISCLOSURE

5 **APPARATUS AND METHOD FOR ENCRYPTING AND DECRYPTING DATA WITH INCREMENTAL DATA VALIDATION**

An apparatus and method for encrypting and decrypting data with incremental data validation is provided. With the

10 apparatus and method, data is encrypted and a digital digest is generated in chunks. That is, the digital digest is comprised of a plurality of intermediate digital digest chunks, each of which can be used to validate a portion of the associated encrypted data. During decryption, a portion

15 of the encrypted data is read and decrypted at approximately the same time that a digital digest is calculated for that portion of the encrypted data. The calculated digital digest may then be compared to an intermediate digital digest associated with the portion of the encrypted data,

20 and which is appended to the encrypted data. If the two digital digests match, decryption of the encrypted data may proceed to the next portion of the encrypted data. If the two digital digests do not match, decryption is halted and the data message or packet is discarded without having

25 decrypted the entire data message or packet. In this way, resources may be freed from processing non-authentic data messages or packets so that they may be used in processing authentic data messages. Thus, the susceptibility of the present invention to denial of service attacks is noticeably

30 reduced in comparison with the prior art.